AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

Claim 1 (Previously presented): An application authentication system comprising:

a terminal device having no secure information concealing area, said terminal device including an application and application running means; and

a secure device connected fixedly or detachably to said terminal device, said secure device for authenticating the application requesting access to the secure device;

wherein said secure device authenticates the application running means, and then authenticates the application based on a result of a process that the application running means executes on the application.

Claim 2 (Currently amended): The application authentication system according to Claim 1, further comprising:

an Operating System (OS) verifying and invoking said application running means, wherein said application running means is an application execution runtime environment,

wherein an application electronic signature that certifies a validity of the application is attached to the application,

wherein the application running means calculates digest data of the application to which ~~an~~the application electronic signature is attached, and presents the digest data and the application electronic signature to the secure device, and

wherein the secure device verifies the application electronic signature by using the presented digest data, and then authenticates the application if a verified result is normal.

Claim 3 (Currently amended): The application authentication system according to Claim 1, further comprising:

an Operating System (OS) verifying and invoking said application running means, wherein said application running means is an application execution runtime environment; and

a database stored in the secure device, wherein the database includes predetermined digest data for authenticating a plurality of applications,

wherein the application running means calculates digest data of the application and presents the digest data to the secure device, and

wherein the secure device collates the presented digest data with digest data held in the[[a]] database of the secure device, and then authenticates the application if a collated result is normal.

Claim 4 (Currently amended): The application authentication system according to Claim 3,

wherein the application running means calculates digest data of the application and sends out a process request command to the secure device, then

wherein the secure device sends out first information to the application running means, then

wherein the application running means encrypts the first information by using the digest data and sends out encrypted information to the secure device, and then

wherein the secure device decrypts the encrypted information by using the digest data stored in the[[a]] database of said secure device and then collates decrypted information with the first information.

Claim 5 (Currently amended): The application authentication system according to Claim 1, further comprising:

an Operating System (OS) verifying and invoking said application running means, wherein said application running means is an application execution runtime environment,

wherein the application running means verifies an electronic signature of the application to which the electronic signature is attached to authenticate the application, and

wherein the secure device accepts an authenticated result of the application running means to authenticate the application.

Claim 6 (Original): The application authentication system according to Claim 2,

wherein the secure device 1) shares a second information with the application running means if the secure device authenticates the application running means, and 2) accepts a process request if the second information are added to the process request issued from the application that the secure device authenticates.

Claim 7 (Previously presented): A secure device connected fixedly or detachably to a terminal device, said secure device comprising:

a card manager for executing a process of authenticating the terminal device; and

a card application for applying an authenticating process to an access request application stored in the terminal device;

wherein the terminal device has no secure information concealing area, and

wherein the card application authenticates the application based on a process that is applied to the application by the terminal device, then confirms that the process of authenticating the terminal by the card manager is completed, and then accepts an access request of the authenticated application.

Claim 8 (Currently amended): A terminal device including:

an application execution runtime environment~~running means~~;

an Operating System (OS) verifying and invoking the application execution runtime environment; and

an application stored in the terminal device and executed by the application execution runtime environment,

wherein the terminal device has no secure information concealing area, and

wherein the application execution runtime environment~~running means~~ calculates digest data of the application to request an access to a fitted secure device after the fitted secure device authenticates the application execution runtime environment~~running means~~, then authenticates the application by using the digest data, and then issues an access request to the secure device.

Claim 9 (Currently amended): The terminal device according to Claim 8,

wherein the application execution runtime environment~~running means~~ verifies an electronic signature attached to the application by using the digest data, and authenticates the application.

Claim 10 (Currently amended): The terminal device according to Claim 8,

wherein the application execution runtime environment~~running means~~ sends out the digest data to the secure device, then acquires a collated result of the digest data from the secure device, and then authenticates the application.

Claim 11 (Currently amended): An application authentication system comprising:

a terminal device having no secure information concealing area; and

a secure device connected fixedly or detachably to said terminal device;

wherein said terminal device includes ~~1)~~ applications, ~~and 2)~~ an application execution runtime environment~~running means~~ for running and authenticating the applications requesting access to the secure device, and an Operating System (OS) verifying and invoking the application execution runtime environment; and

wherein said secure device authenticates an application stored in the terminal device in order to permit access to said secure device, if the application is authenticated by application execution runtime environment, which is~~running means~~ authenticated by said secure device, and

wherein the application execution runtime environment calculates digest data of said application and verifies an electronic signature attached to the application by using the digest data, and authenticates the application.

Claim 12 (Currently amended): A terminal, comprising:

an application storage unit storing at least an application;

an application execution runtime environment verifying and executing said application;

an Operating System (OS) verifying and invoking said application execution environment;

a Basic Input Output System (BIOS) verifying and invoking said OS; and

a secure device verifying said BIOS, wherein the application execution runtime environment transmits data including a hash of said application to the secure device and the secure device verifies a validity of the hash of said application.

Claim 13 (Currently amended): A method of verification of an application on a terminal, comprising the steps of:

verifying a Basic Input Output System (BIOS) by a secure device;

verifying and invoking an Operating System (OS) by the BIOS;

verifying and invoking an application execution runtime environment by the OS;

verifying an executing the application stored in an application storage unit of the terminal by the application execution runtime environment; and

transmitting data including a hash of said application to the secure device by the application execution runtime environment; and

verifying a validity of the received hash of the application by the secure device.